WE CLAIM:

1. A software protection system for use in a computer having a memory, the system comprising:

a protection device connectable to the computer;

a computer program having at least a first portion thereof to be stored in the computer and at least a second portion thereof stored in the protection device;

a flow of I/O communications between the computer and the protection device;

means in the protection device for executing the second portion of the program contained in the device, wherein the execution of the second portion of the program is carried out by sharing the memory and resources of the computer, and wherein the computer and the protection device operate together and by using the first and second portions of the computer program to execute the computing program.

2. The system of claim 1, wherein the first portion of the computer program comprises a plurality of first program modules and the second portion of the computer program comprises a plurality of second program modules, wherein the first program modules include call instructions

for execution of the second modules in the protection device.

3. The system of claim 2, wherein the second modules contain control transfer instructions for directing the execution of the program to the first modules in the computer and/or between modules in the protection device.

4. The system of claim 1, wherein the protecting device comprises a physically secure microprocessor, a volatile memory and a non volatile memory having the second program modules stored therein, the non volatile memory being non readable from outside the device.

5. The system of claim 2, wherein the second program modules are encrypted and are desencrypted for storing in the protection device.

6. A software protection system for use in a computer having a memory, the system comprising:

a protection device connectable to the computer;

a computer program having at least a first portion thereof for storing into the computer and at least a second portion thereof stored in the protection device, wherein the memory and resources of the computer are shared by the protection device and the computer at least during the

execution of the second program portion stored in the protection device.

7. The system of claim 6, wherein the second portion of the program comprises modules of the machine code of the program, the protection device comprises at least one physically secure microprocessor, a volatile memory and a non volatile memory; communication means between the computer and the protection device; and an interface program providing an interface between the computer and the protection device.

8. The system of claim 1, wherein the protection device is a tamper proof device.

9. The system of claim 1, wherein the computer program includes timer means for providing a limited period of time of use of the program.

10. The system of claim 1, wherein the computer program includes interface means for providing a communication flow between the computer and the protection device.

11. The system of claim 1, wherein the computer program to be protected is a program used in a under-

license net wherein the number of programs to be executed in the net is restricted.

12. A method for protecting a computer program against the unauthorized copy and/or use thereof, the method comprising:

providing a protection device for connecting to a computer having a memory;

providing the computer program with at least a first portion thereof for storing into the computer and at least a second portion thereof stored in the protection device;

sharing the memory of the computer between the computer and the protection device; and

operating the protection device and the computer together to execute the computer program, whereby the first and second portions of the computer program are executed by sharing computer resources.

13. The method of claim 12, wherein the step of providing the computer program with at least a first portion for storing into the computer and at least a second portion stored in the protection device comprises forming the first portion of the program by removing from the computer program at least one module consisting of a machine code, storing the at least one removed module into

the protection device to form the second portion of the program, storing in the first portion of the program a calling module including function calls for the execution of the at least one module that was removed from the program and stored in the protection device, wherein the calling module replaces the at least one module removed from the program.

14. The method of claim 13, wherein the step of executing the computer program comprises executing the first portion of the program in the computer, operating the calling module for executing at least one module of the second portion of the program in the protection device, and interchanging communications in a manner to prevent the cracking thereof.

15. The method of claim 14, wherein the modules in the protection device include instructions for interrupting and routing the execution of the computer program, instructions acceding to external variables and instructions that are combined in a complex manner to prevent the cracking thereof.

16. The method of claim 13, wherein the step of forming the first portion of the program by removing from the computer program at least one module comprises removing

a plurality of modules for storing into the protection device to form the second portion of the program, wherein a plurality of calling modules are stored in the first portion of the program for replacing the modules removed therefrom, and the step of operating the protection device and the computer comprises the execution of control transfer instructions in the device for directing the execution of the program to the first modules in the computer and/or between modules in the protection device.

17. The method of claim 16, wherein the step of removing modules from the computer program comprises selecting the modules containing at least control transfer instructions, instructions accessing to external variables and non-inferable instructions and removing the modules.

18. The method of claim 17, wherein the modules are automatically removed.

19. The method of claim 12, wherein the step of operating the protection device and the computer together to execute the computer program comprises operating the protection device to execute the portion of the program contained therein by emulating one of the computer processor and the virtual machines JAVA and NET.

20. The method of claim 12, wherein the step of providing the computer program with at least a first portion and a second portion comprises removing at least one module of a plurality of modules of the program, with the at least one module comprising the machine code of the program to be protected and being selected in a manner that that the at least one module contains at least one of instructions for interrupting and directing or routing the execution of the program, instructions accessing outer variables and instructions that when grouped are mostly difficult to be inferred or cracked; storing the removed at least one module into the protection device, the device being non readable from outside; and replacing said at least one removed module by a call module for calling to the execution of the at least one module that has been stored into the device; and the step of operating the protection device and the computer comprises executing the call modules in the computer, whereby the call instructions execute the modules in the device; and executing the at least one module in the protection device by using the memory and resources of the computer and returning the execution to the computer once the at least one module of the protection device has been executed.